

Fig. 1

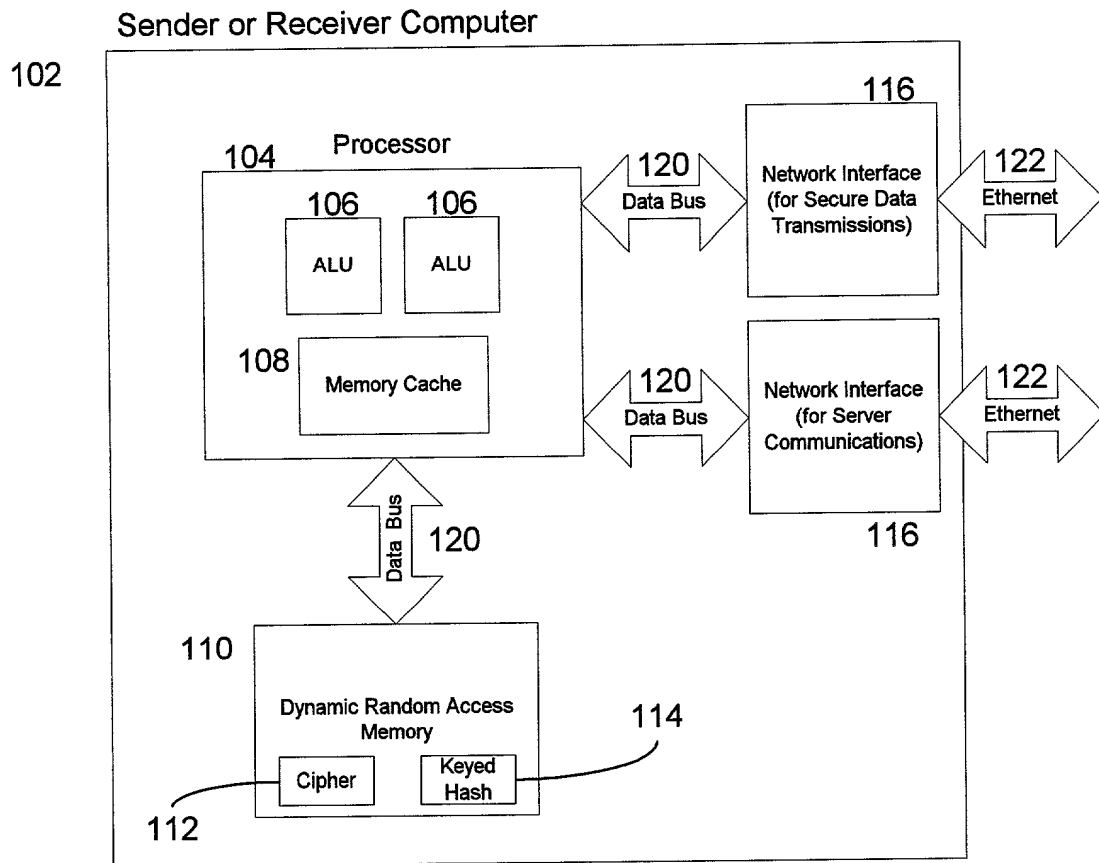
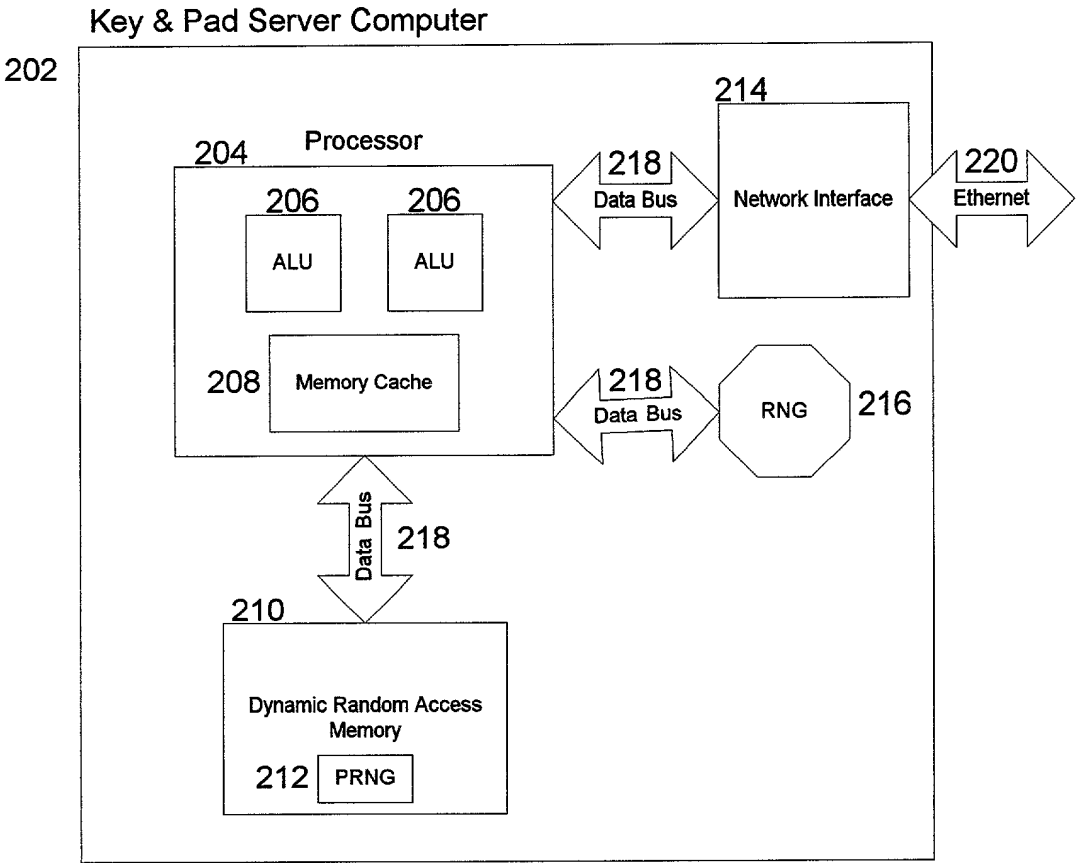


Fig. 2



Simple Mechanism of Generating a Random Permutation of a Sequence of Unique Numbers from 0 to N

Fig. 3

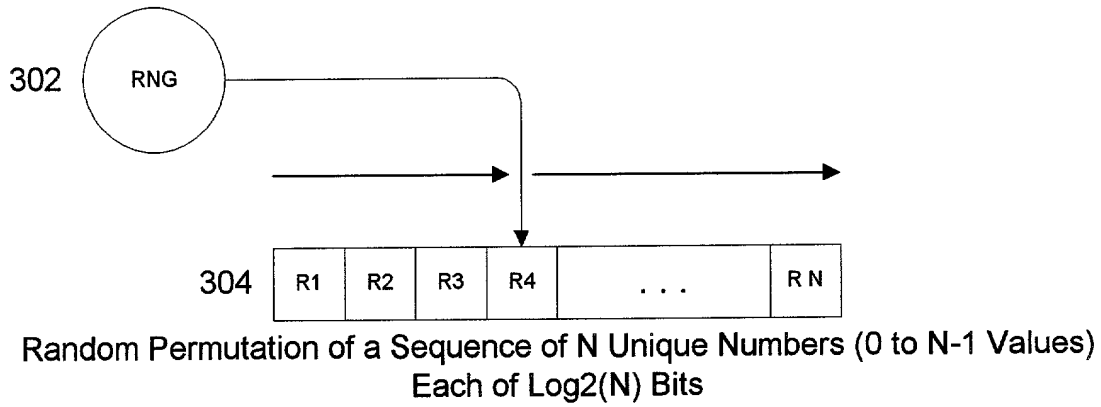


Fig. 4

Near Perfect Riffle Shuffle Mechanism of Generating a Random Permutation of a Sequence of Unique Numbers from 0 to N.

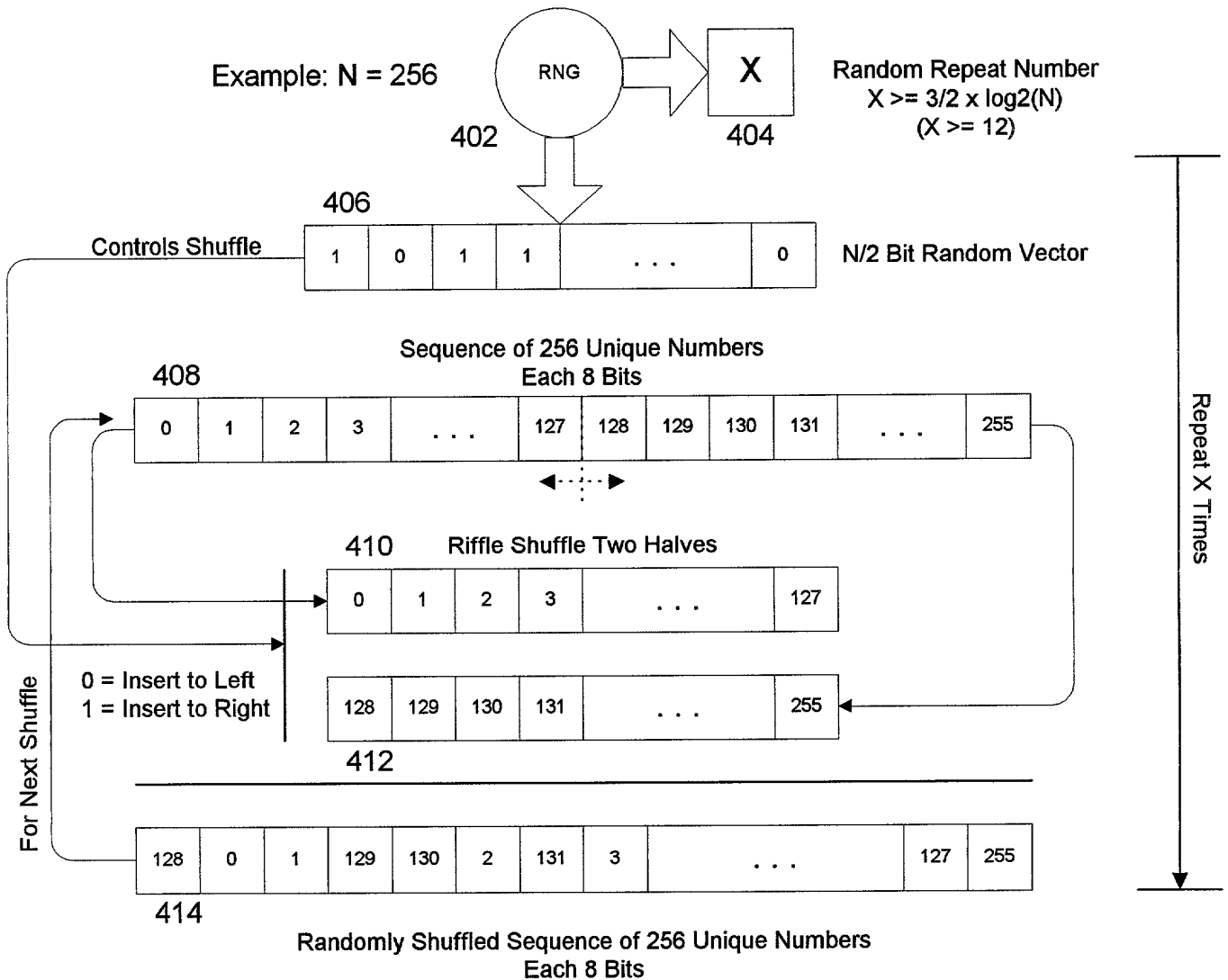


Fig. 5

Randomly Permutating a Sequence of Numbers

Example: $N = 8$

Random Sequence of Eight 3 bit Unique (0 to 7) Indices

502	2	5	4	0	7	6	1	3
-----	---	---	---	---	---	---	---	---

Sequence of Eight Random Numbers

	0	1	2	3	4	5	6	7
Source:	A	B	C	D	E	F	G	H

504

Result:

C	F	E	A	H	G	B	D
---	---	---	---	---	---	---	---

506

Sequence of Eight Shuffled Random Numbers

Controls
Sequence
Re-Ordering

502 504 506

Fig. 6 Key or Seed Data Structure

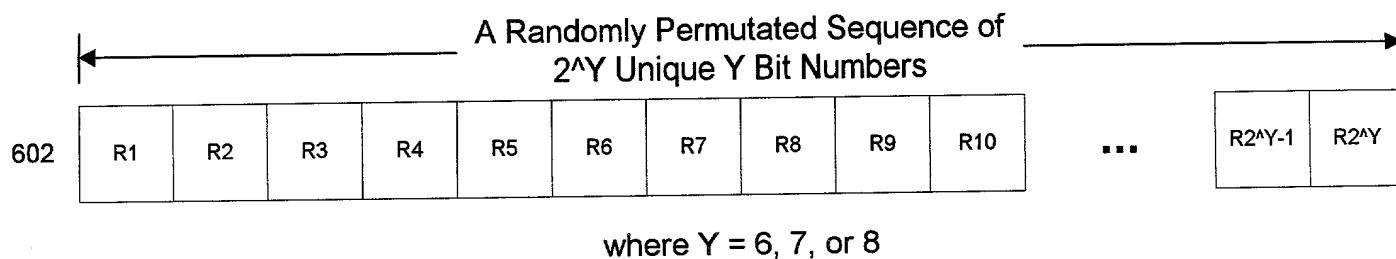


Fig. 7 Unit Sizes Used For Partitioning Random Permutations

702

Card

1 Card = 2^U Bytes, where $U = 0, 1, 2, 3, \text{ or } 4$ (i.e. 1, 2, 4, 8, or 16 Bytes)

704

Pack

1 Pack = 2^V Cards, where $V = 6, 7, 8 \text{ or more}$.

The diagram shows a stack of four overlapping rectangles, each labeled "Card". These are contained within a larger rounded rectangle labeled "Pack". The number "704" is positioned to the left of the "Pack" label.

706

Case

1 Case = 2^W Packs, where $W = 6, 7, 8 \text{ or more}$.

The diagram shows a stack of four overlapping rounded rectangles, each labeled "Pack". These are contained within a larger rectangle labeled "Case". The number "706" is positioned to the left of the "Case" label.

708

Pad

1 Pad or Pool = 2^X Cases, where $X = 6, 7, 8 \text{ or more}$.

The diagram shows a stack of four overlapping rectangles, each labeled "Case". These are contained within a larger rounded rectangle labeled "Pad". The number "708" is positioned to the left of the "Pad" label.

Fig. 8

Flow Chart for Nested Shuffle

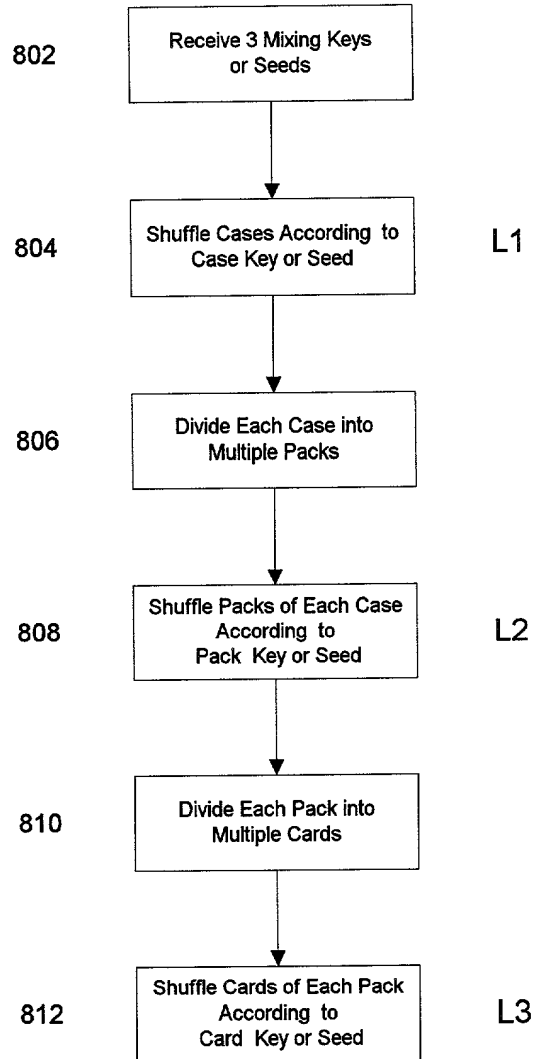


Fig. 9

Nested Shuffle of a Series of Cards

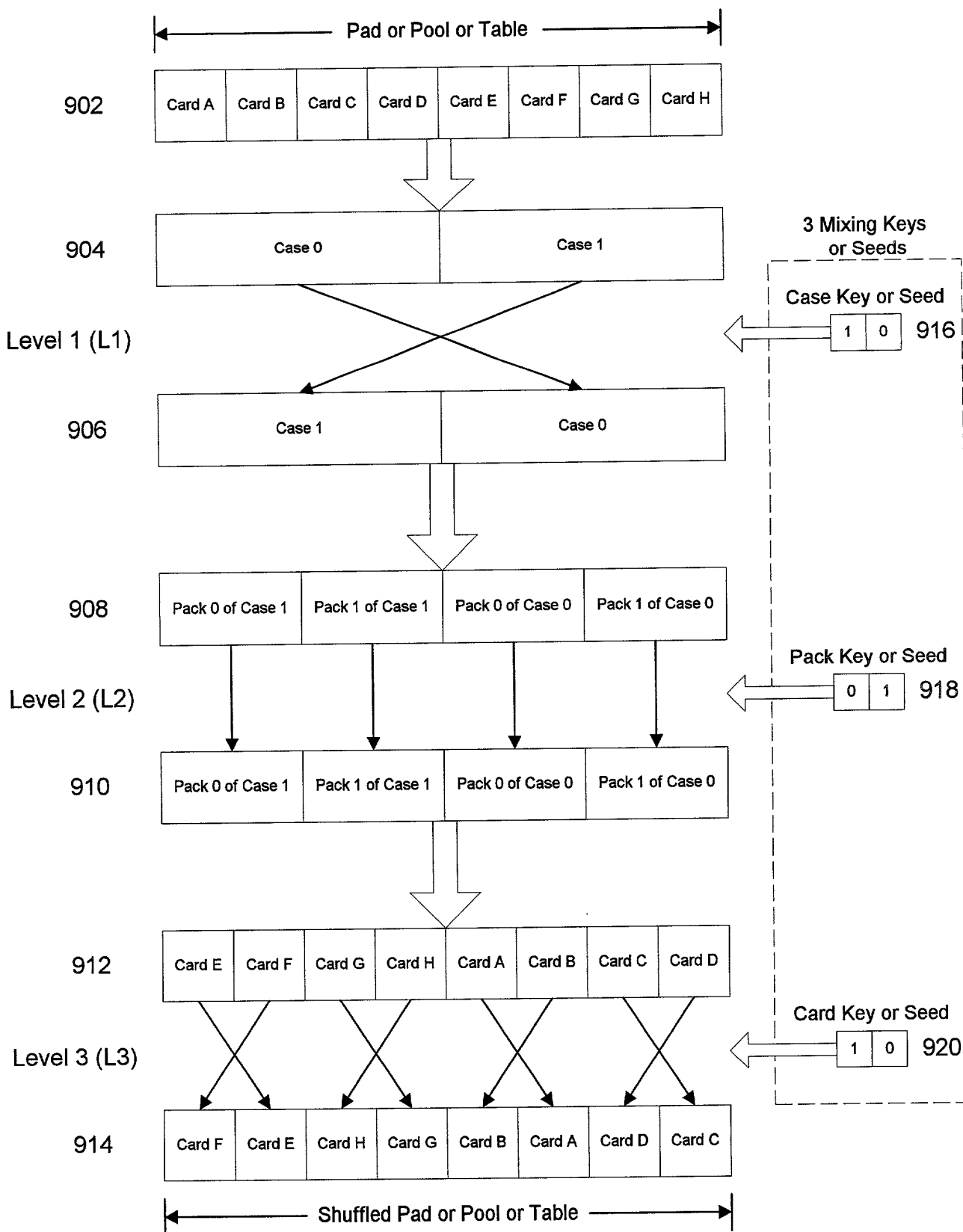


Fig. 10

Non-Cyclic Pseudo-Random Number Generator

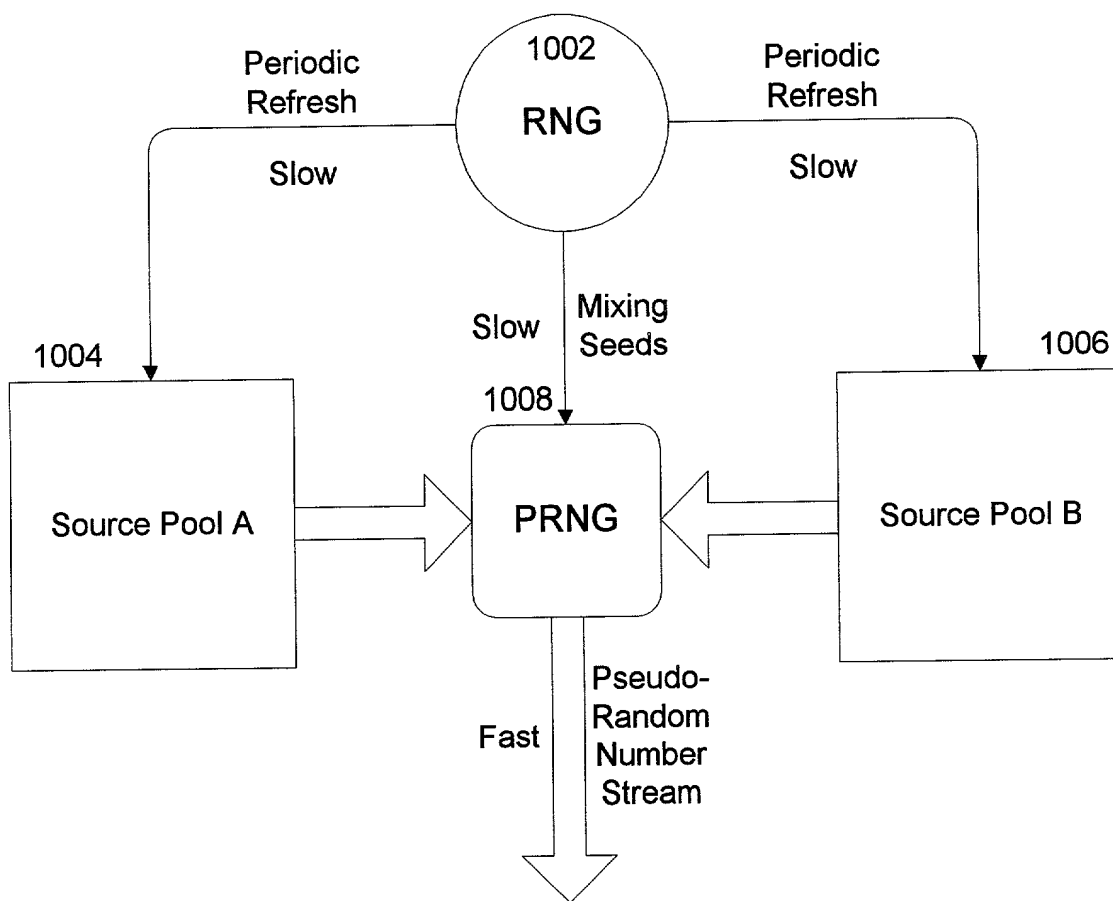


Fig. 11 Non-Cyclic Pseudo-Random Number Generation

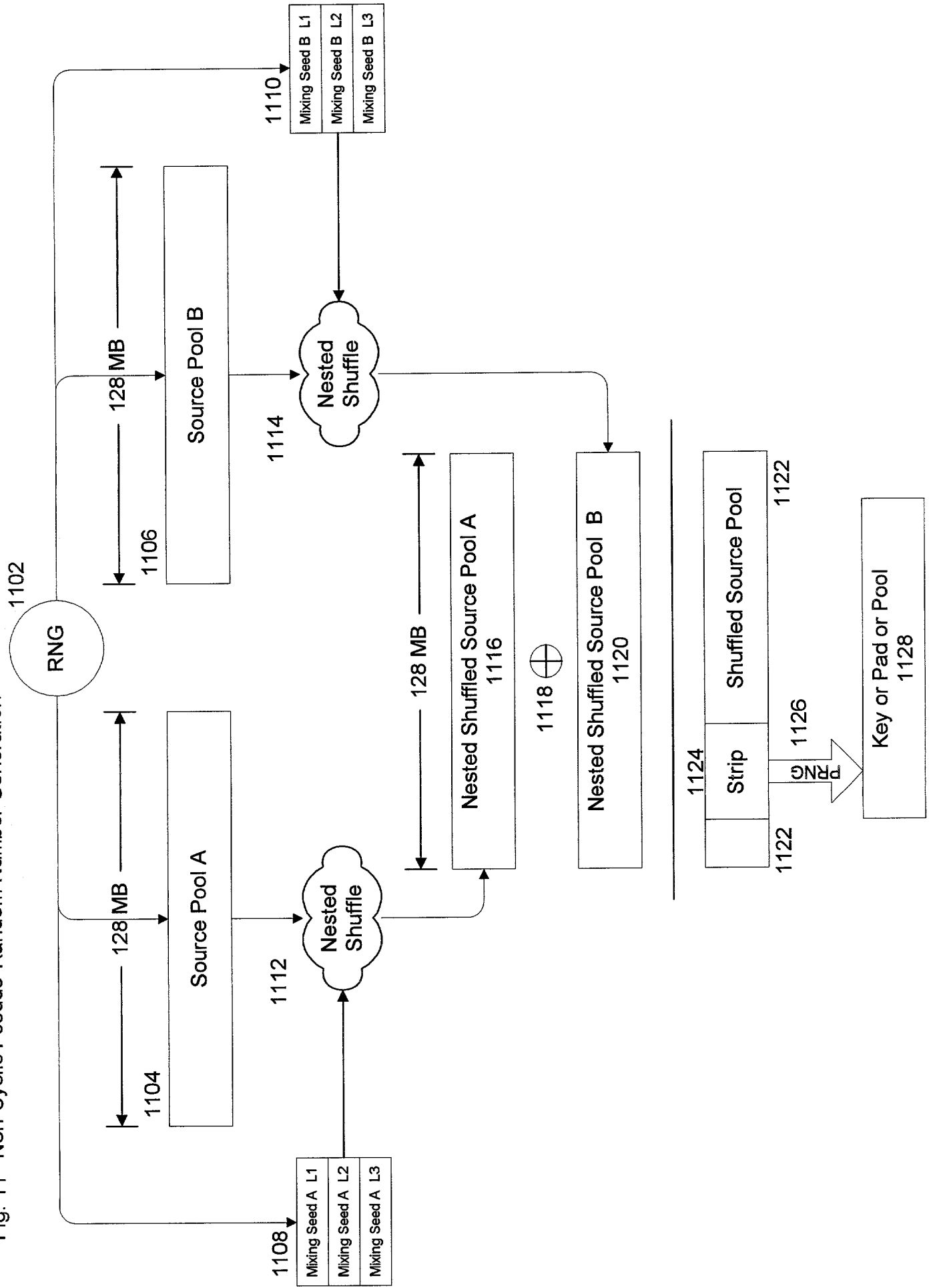


Fig. 12

Nested Shuffle of A Source Pool A or B (128 MB)

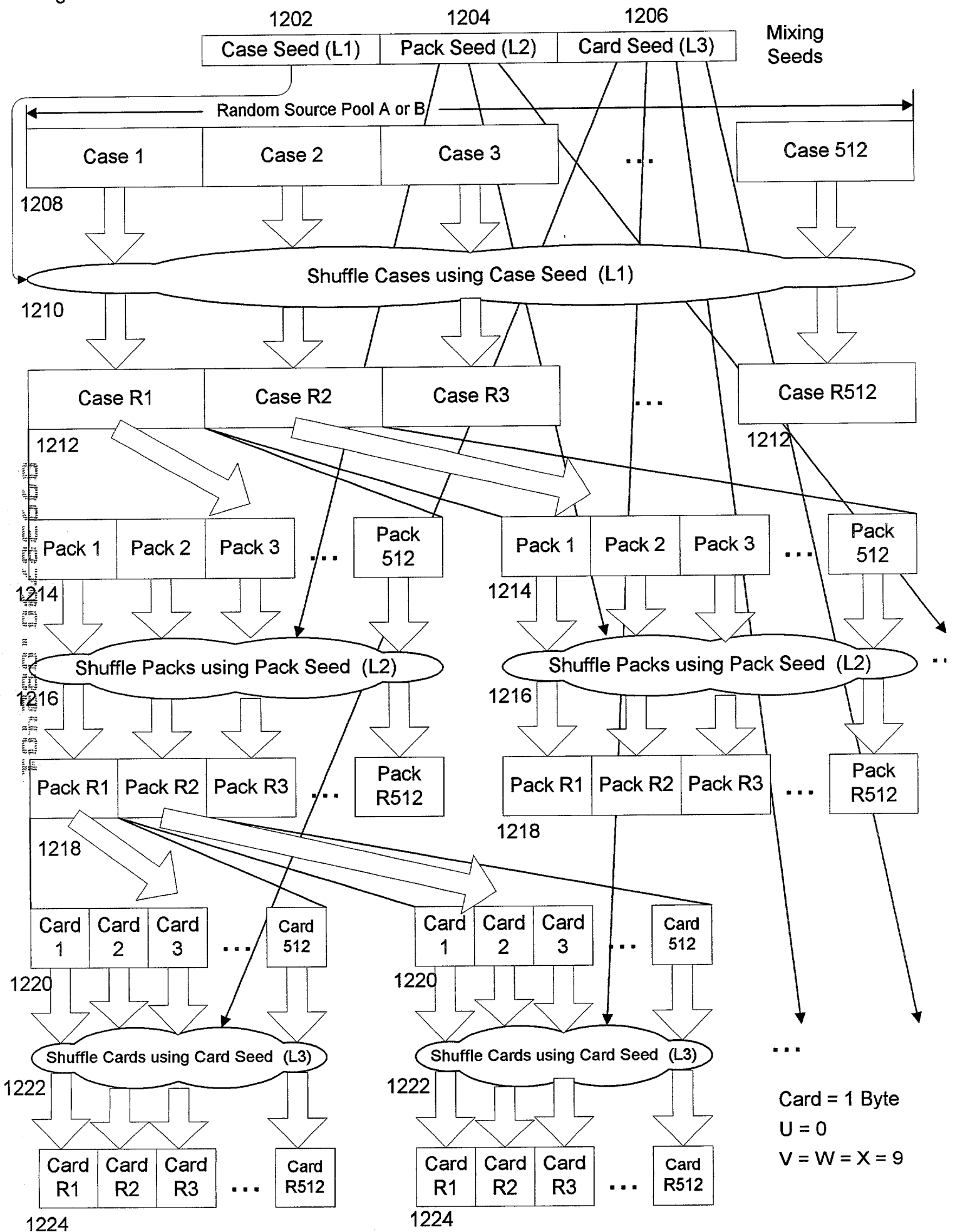


Fig. 13

Keys, Pads and Encrypted
Data Flows
With Central Server

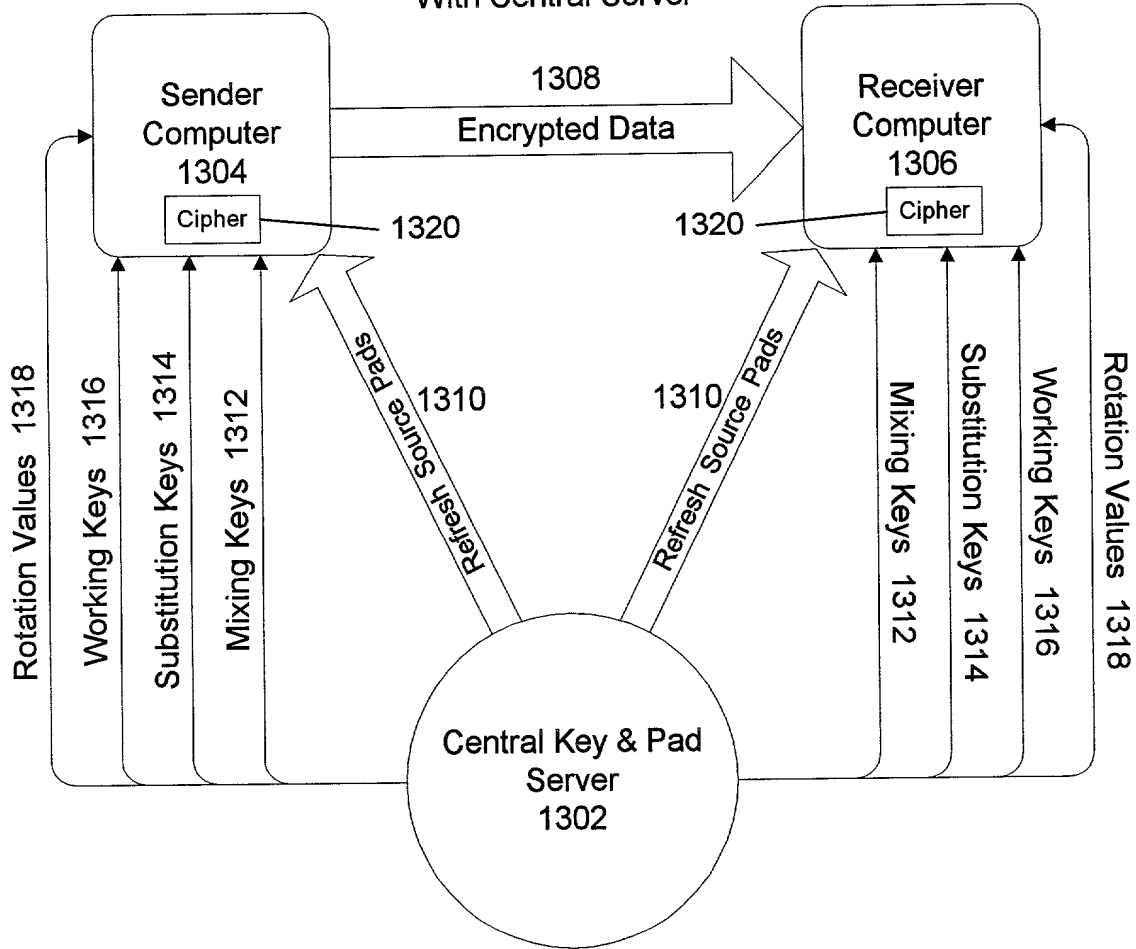


Fig. 14

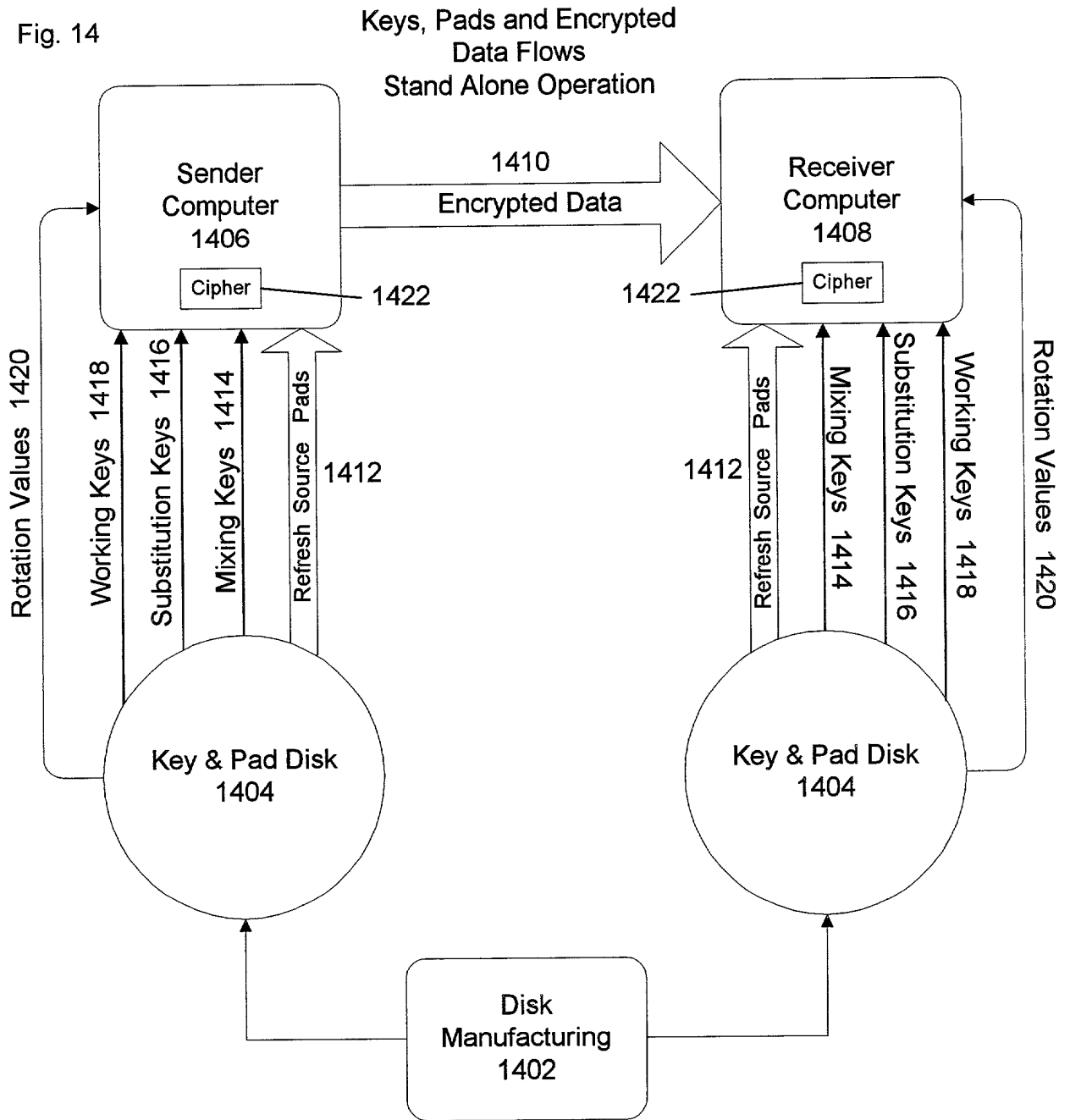


Fig. 15

ENCRYPTION

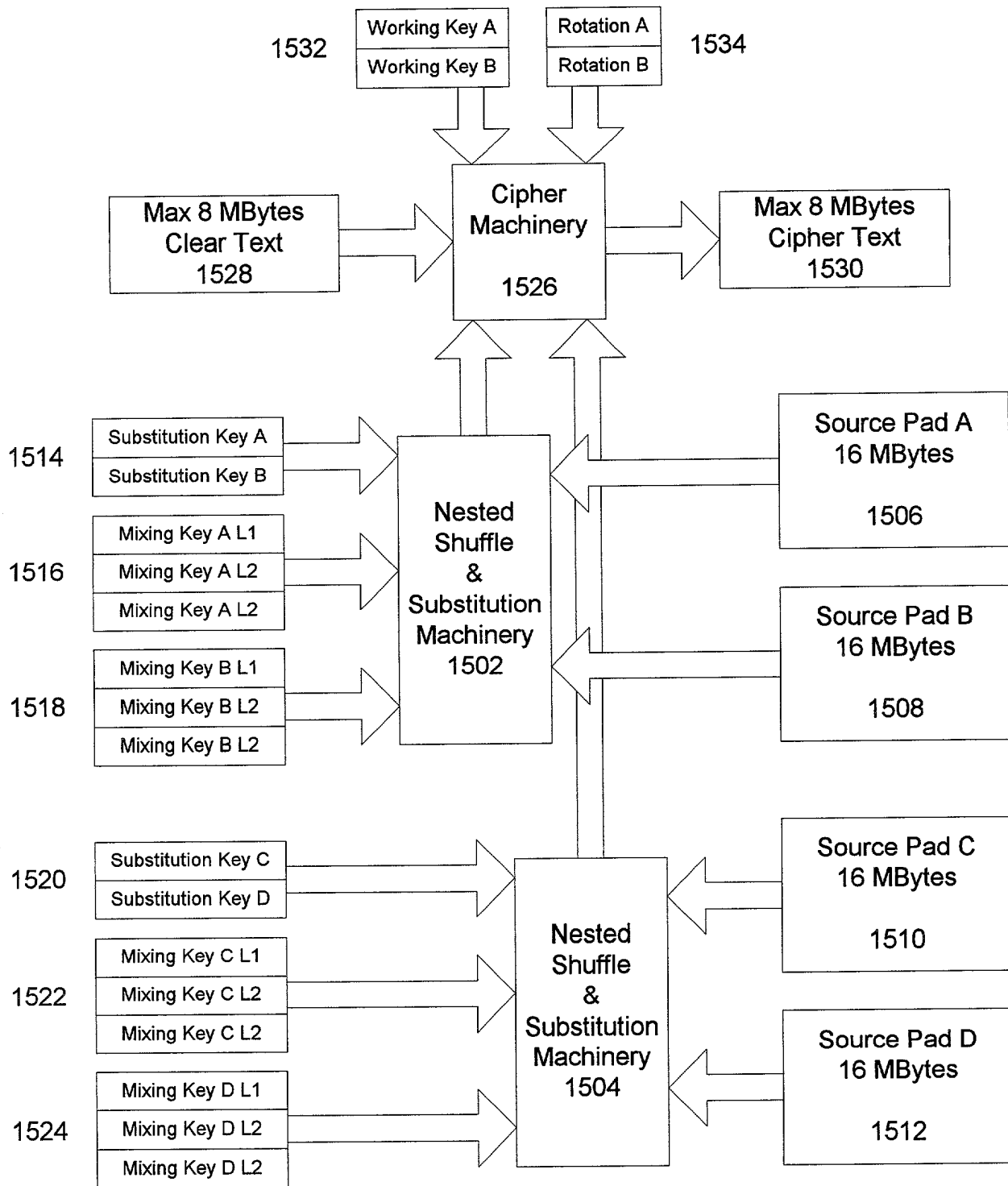


Fig. 16

DECRYPTION

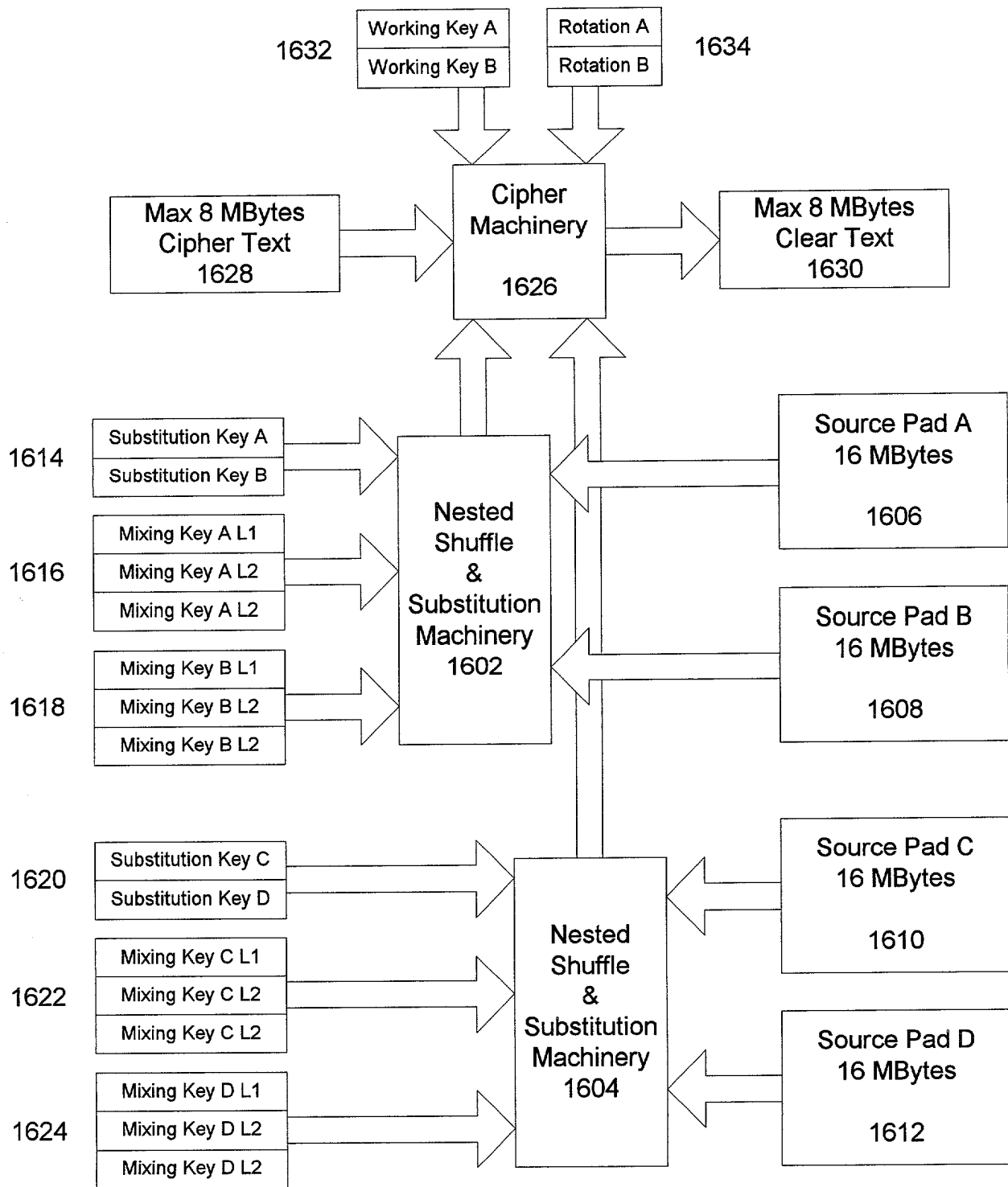


Fig. 17

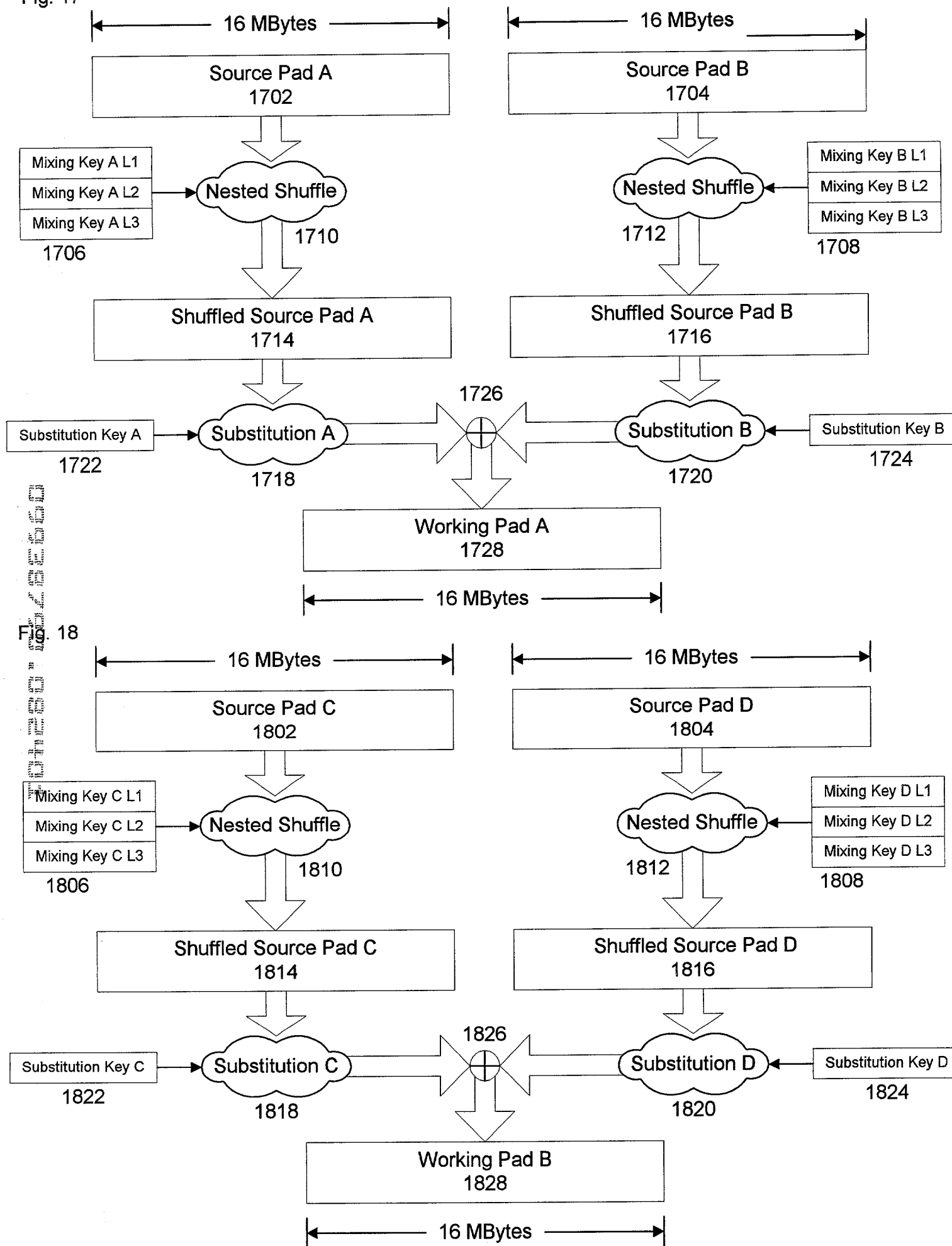


Fig. 19

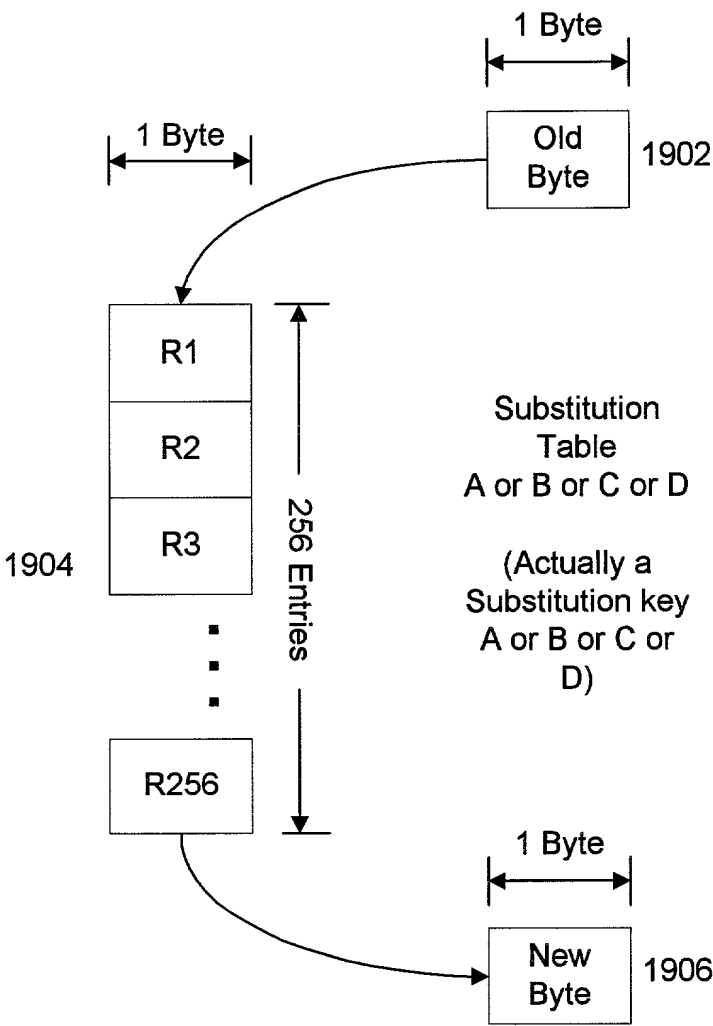


Fig. 20

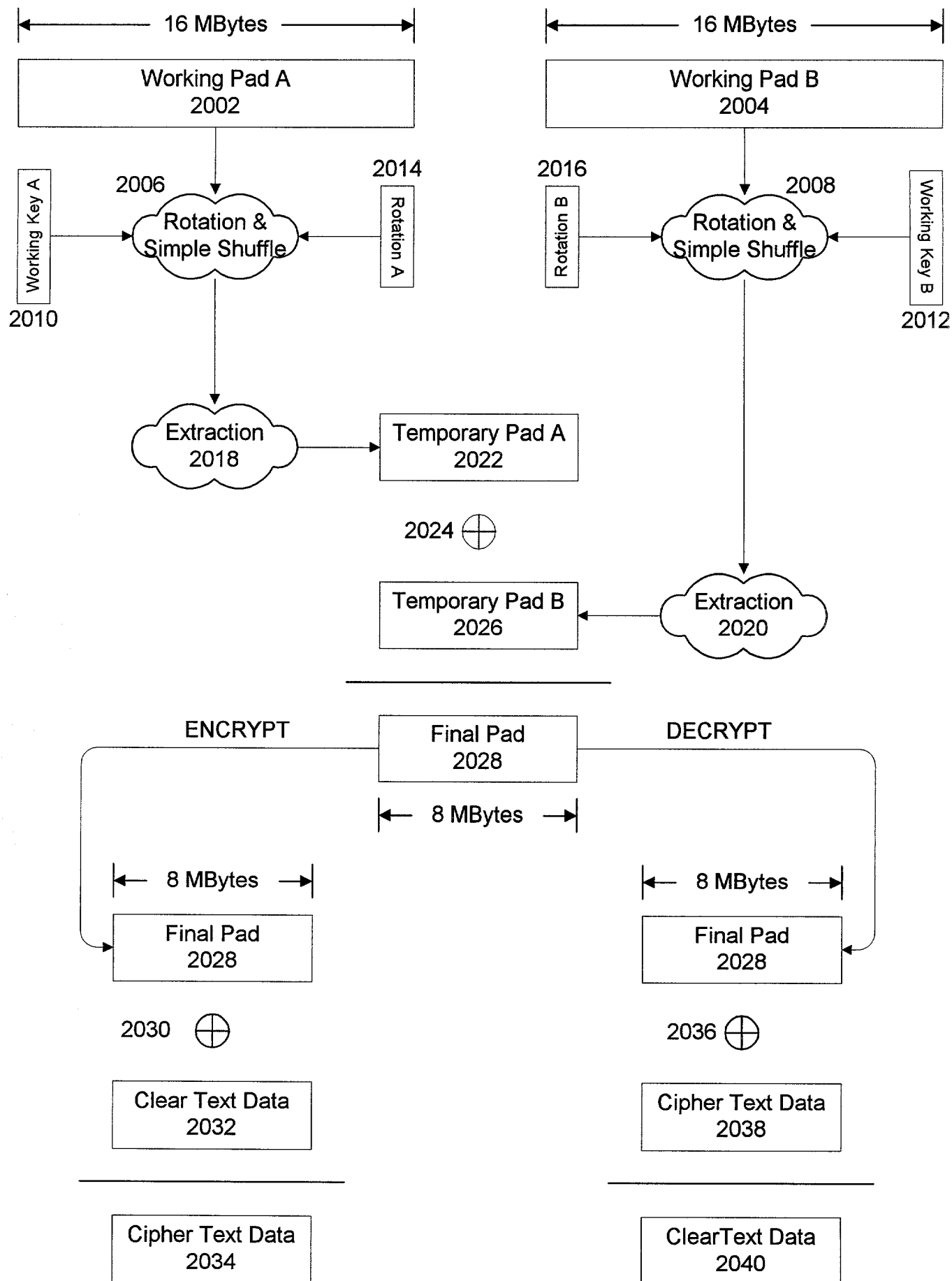


Fig. 21

Nested Shuffle Of A Source Pad (16 MB)

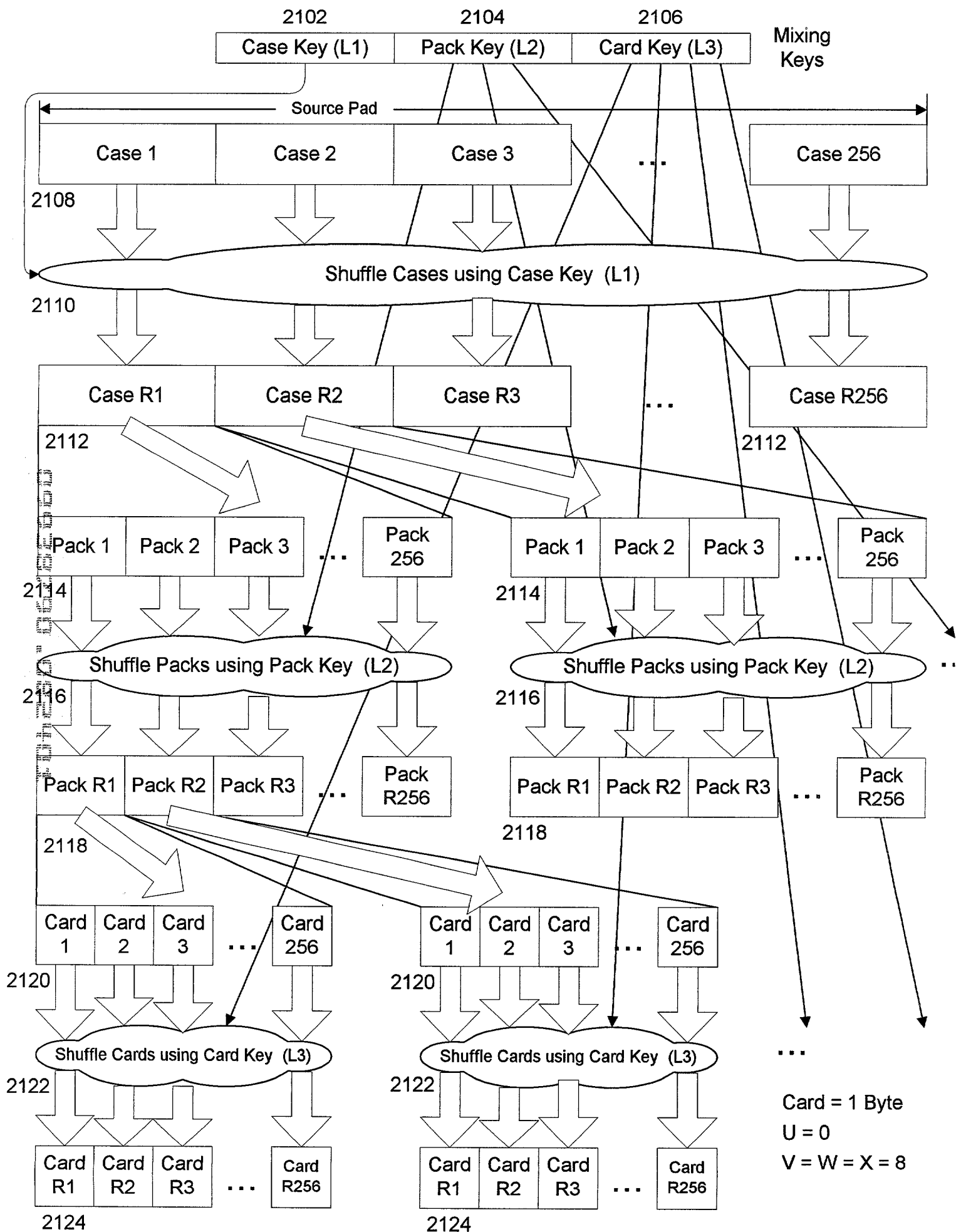


Fig. 22

Rotation & Simple Shuffle of Working Pad (16 MB)
and Extraction of a Temporary Pad (8MB)
Using a Working Key and Rotation Value

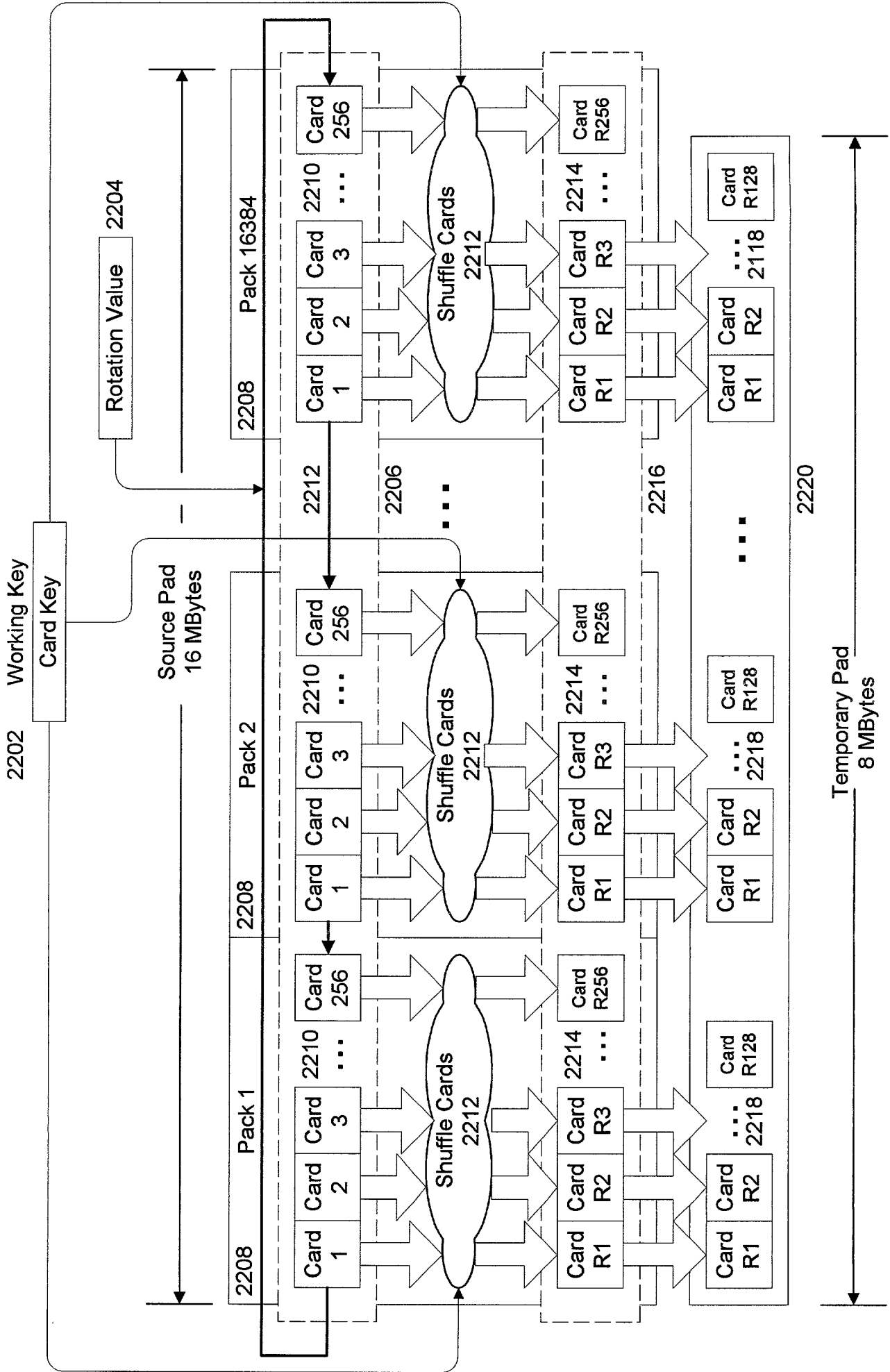


Fig. 23

Keyed One-Way Hash Function

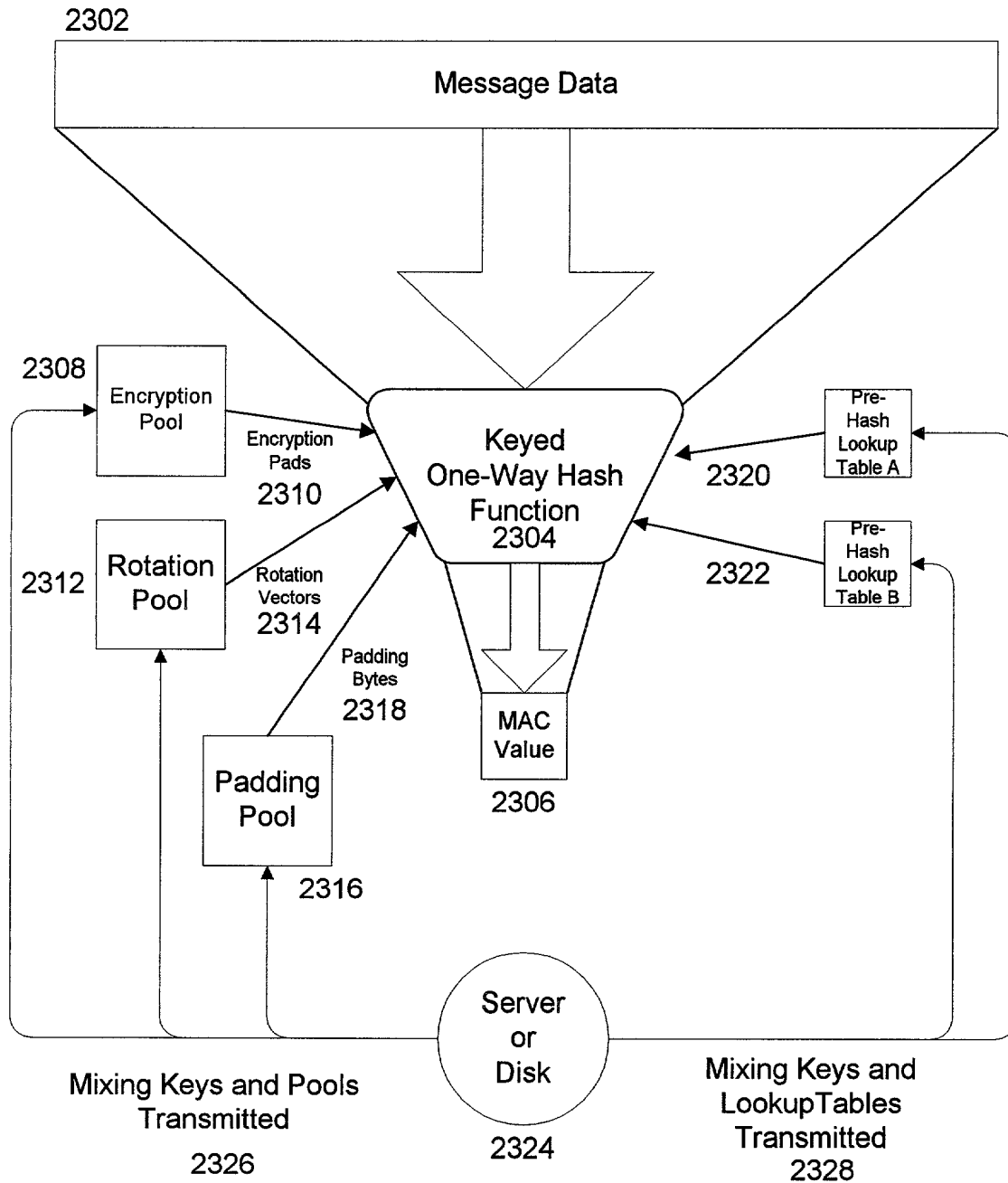


Fig. 24

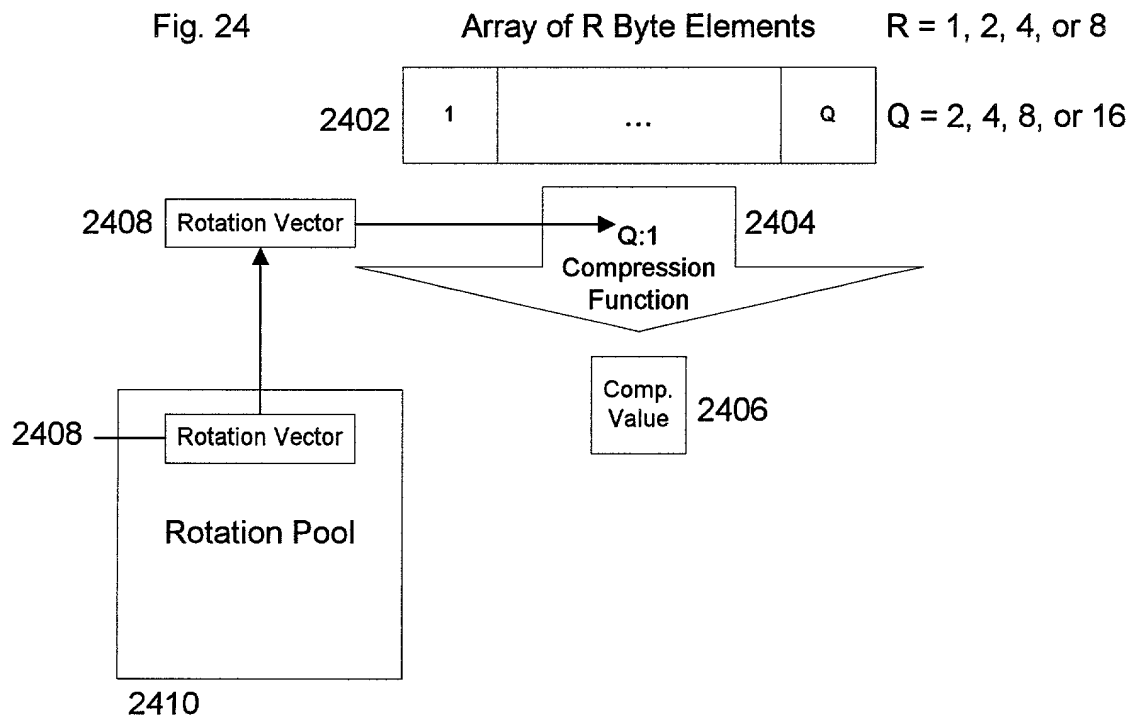


Fig. 25

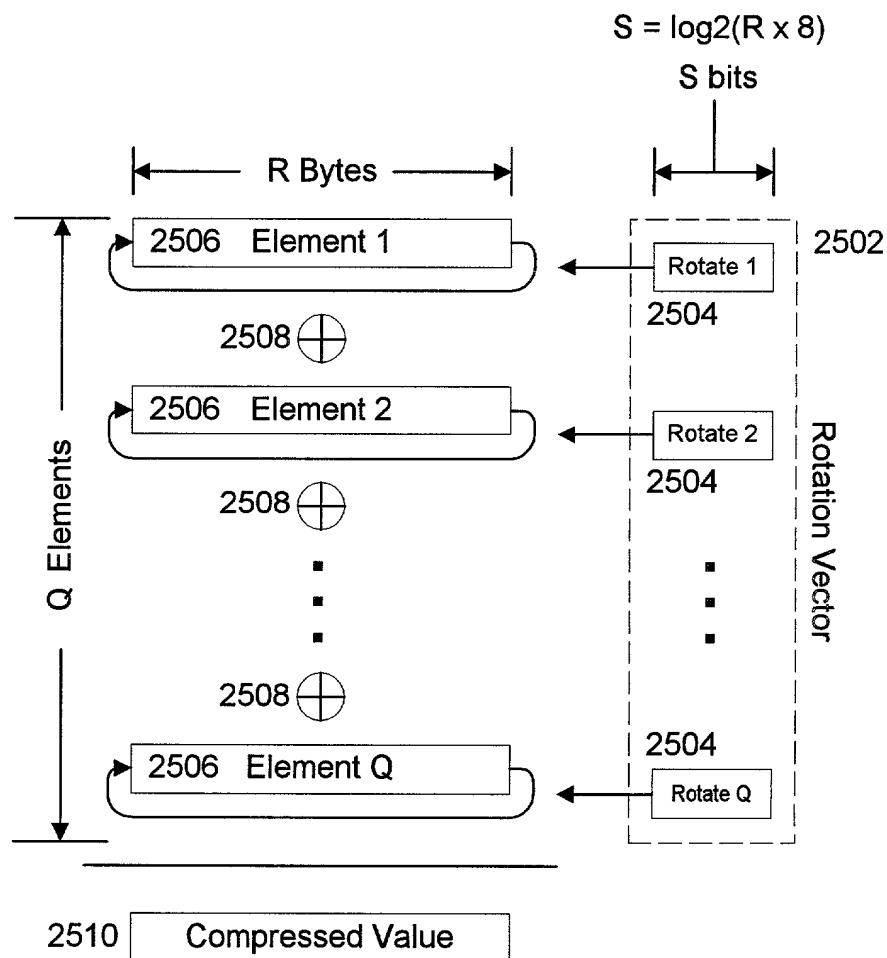


Fig. 26

Compressing a 64 Kilobyte Message

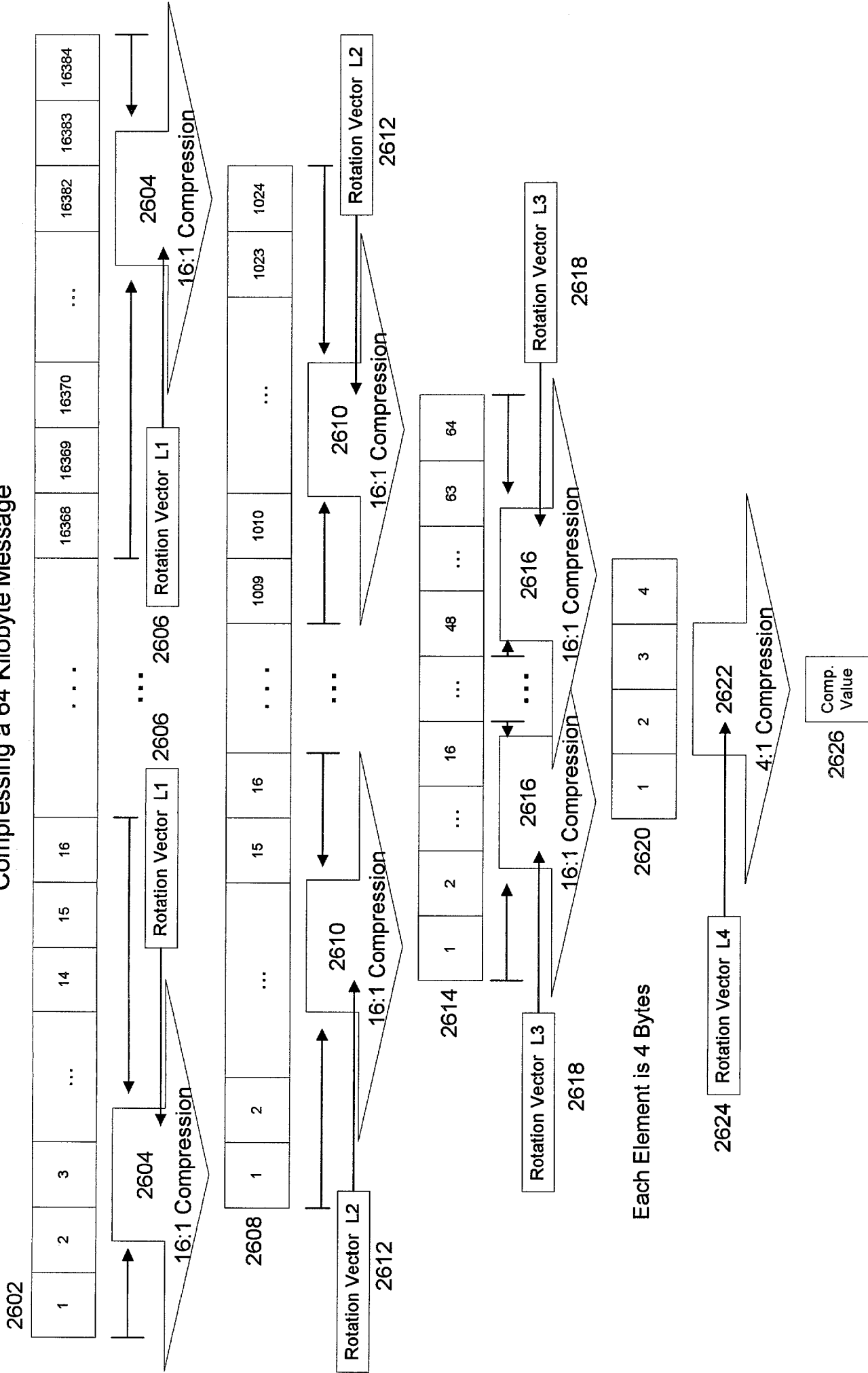


Fig. 27

Compressing a 64 Byte Message

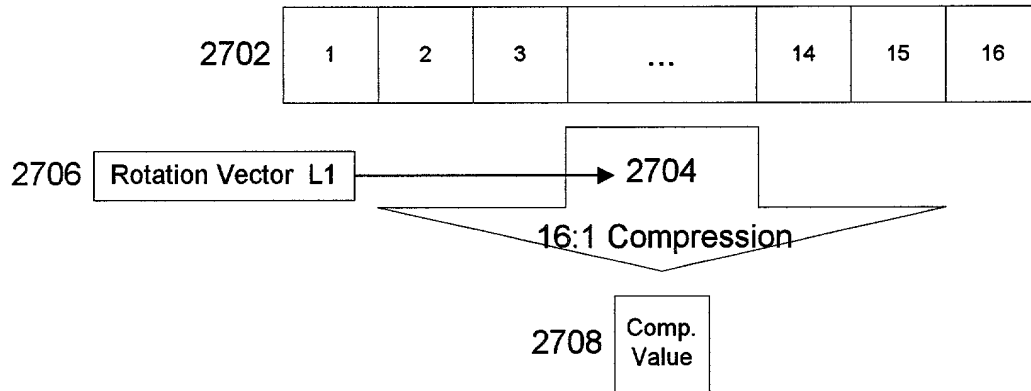


Fig. 28

Compressing a 1518 Byte Message

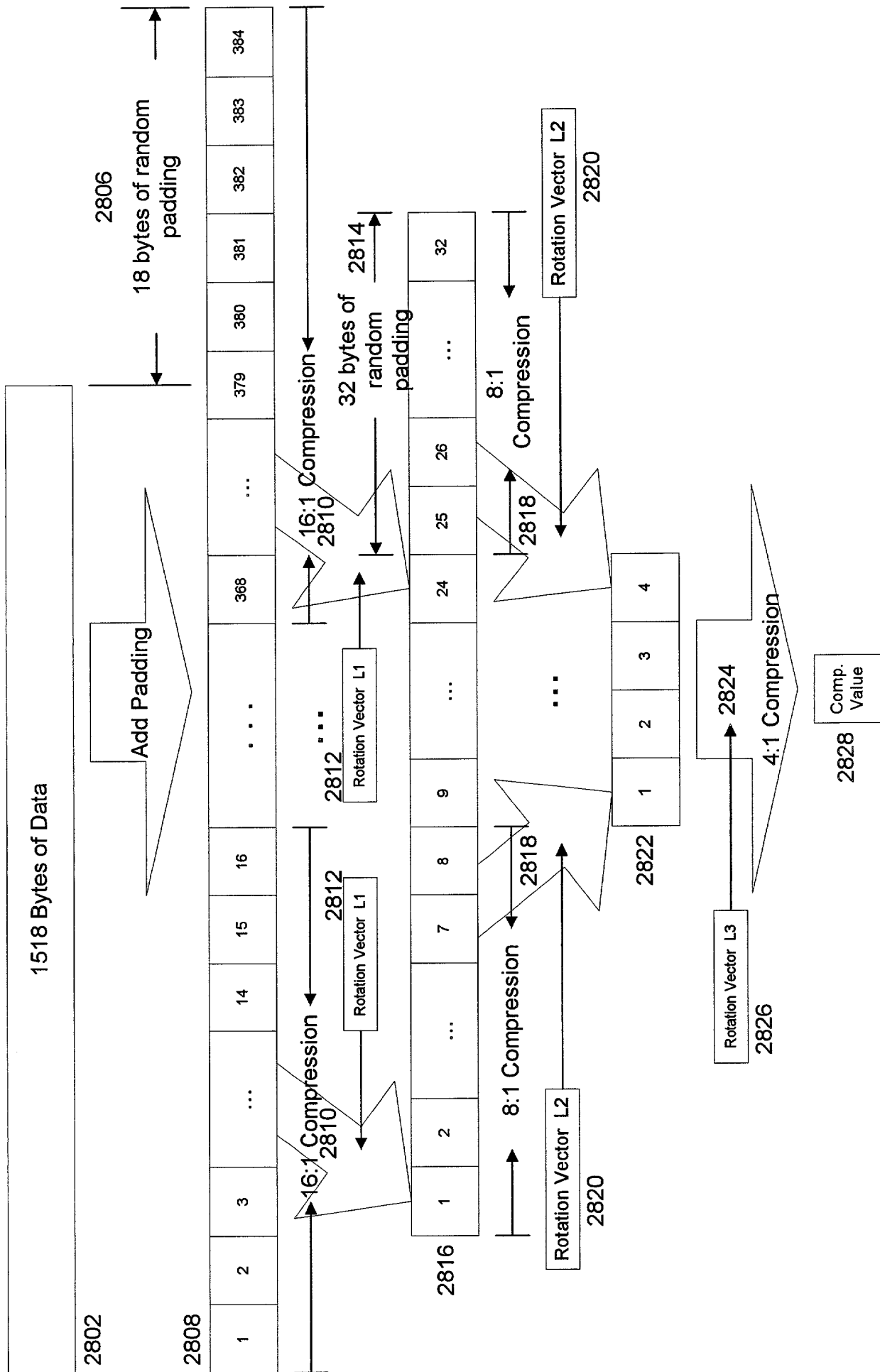
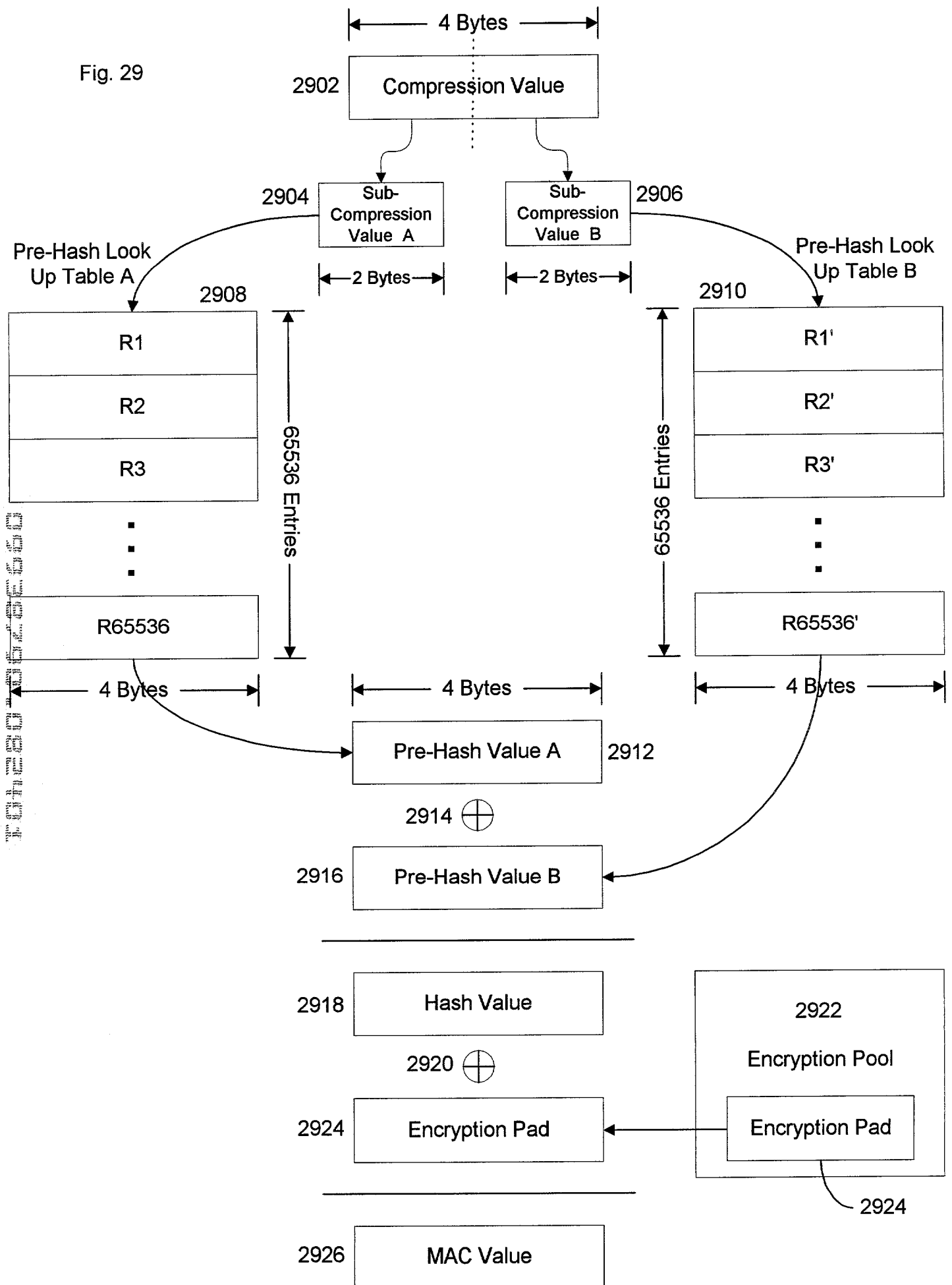


Fig. 29



Nested Shuffling a Pre-Hash Look Up Table (256 KB)

Fig. 30

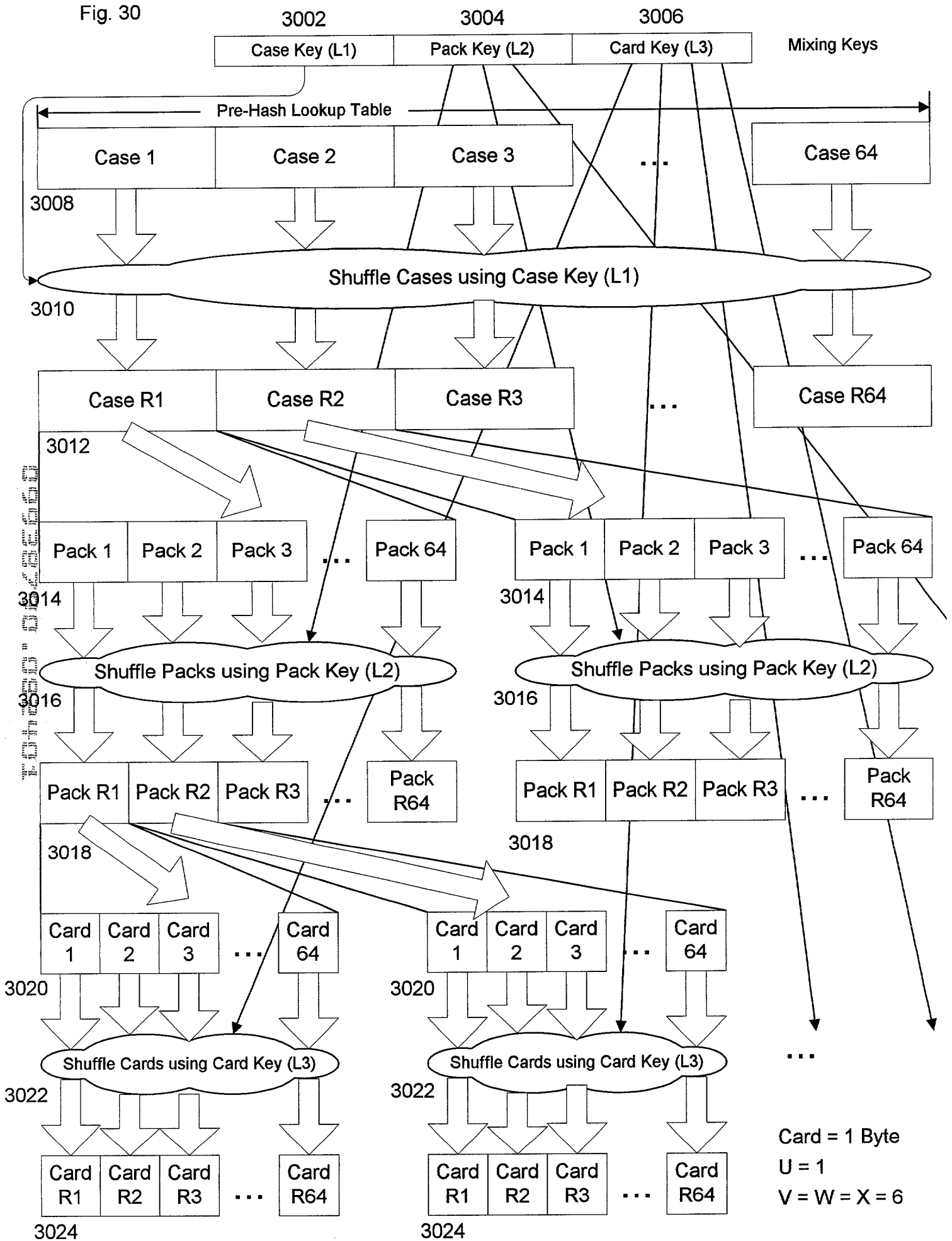


Fig. 31

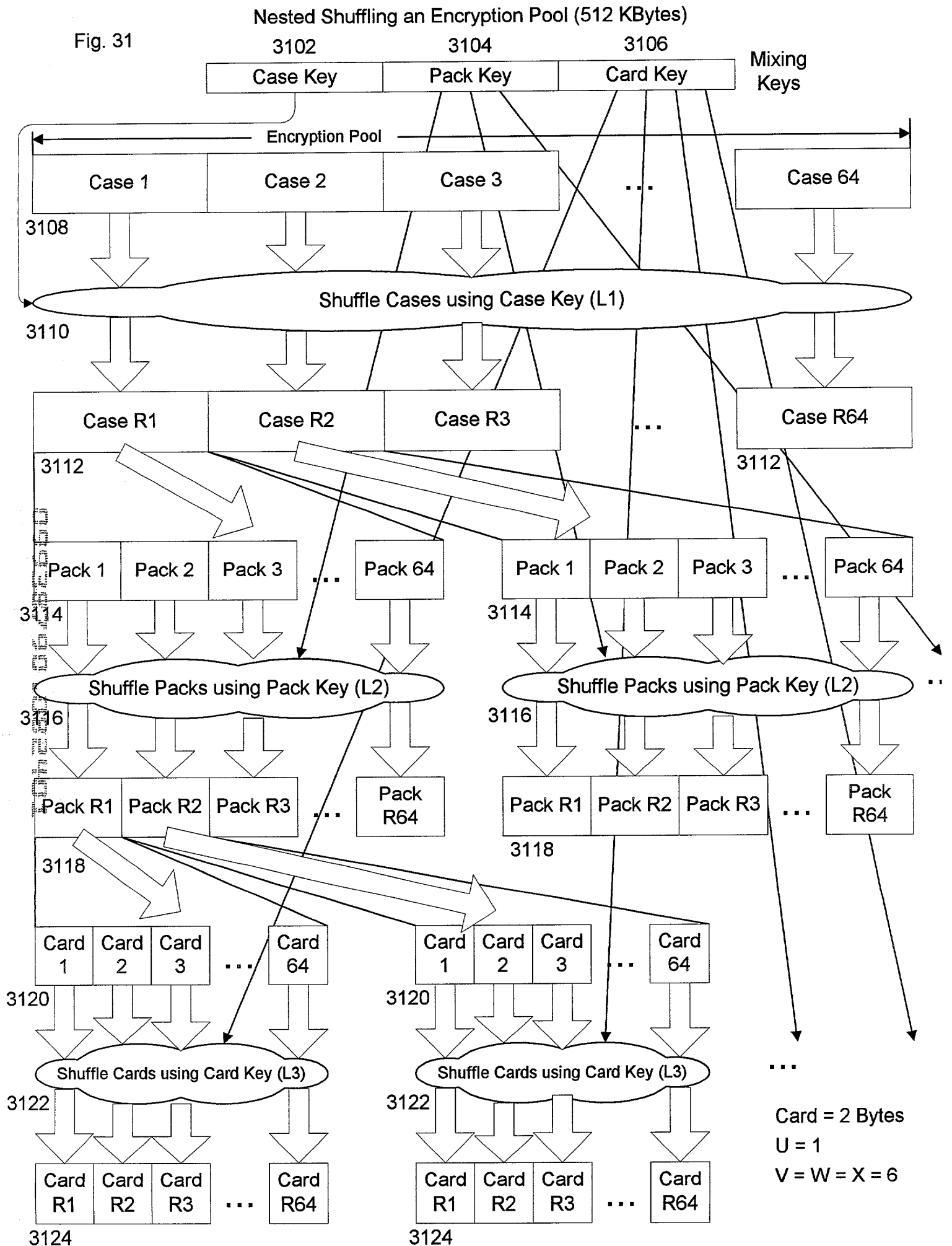
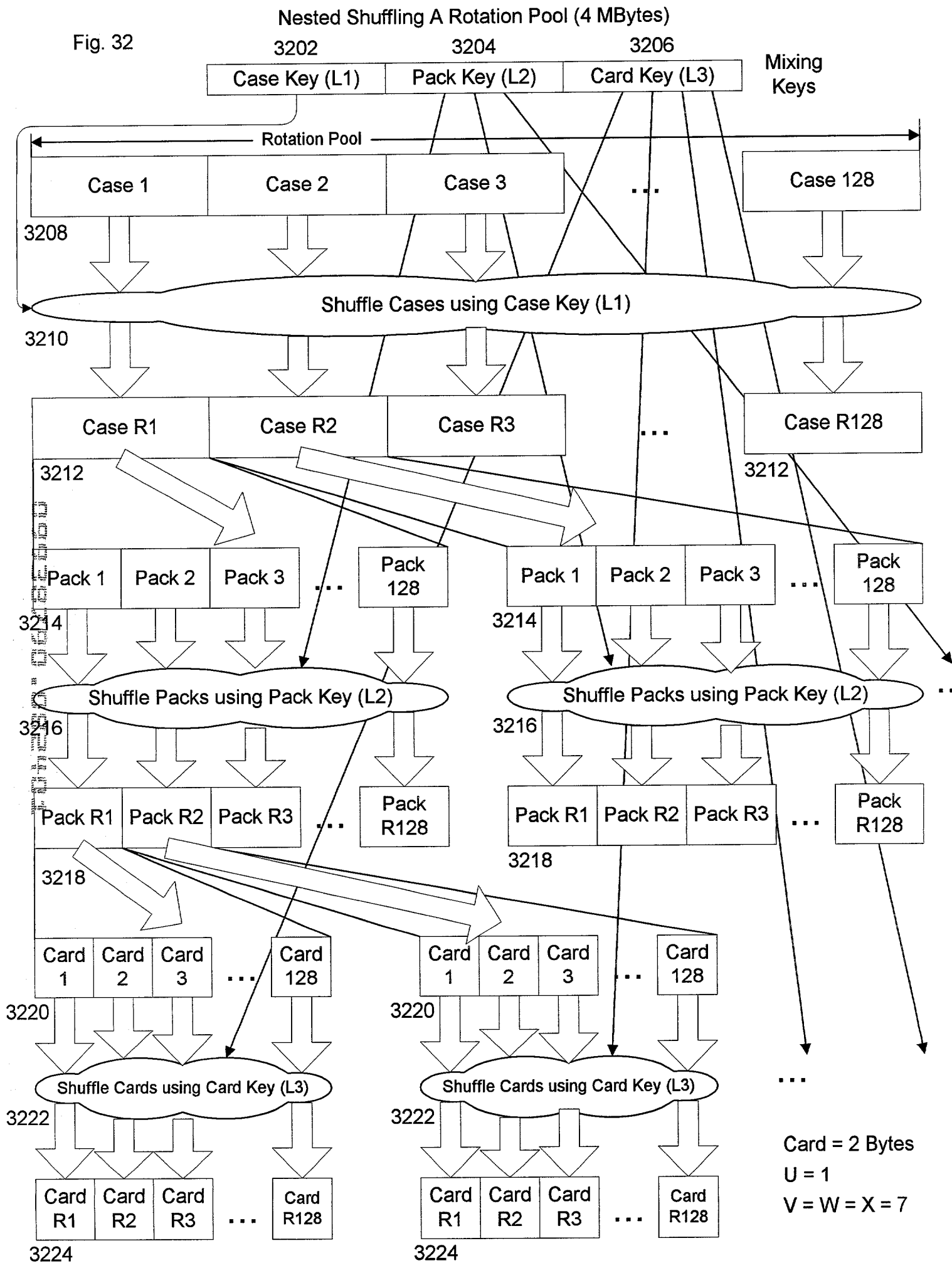


Fig. 32



Shuffling A Padding Pool (256KB)

Fig. 33

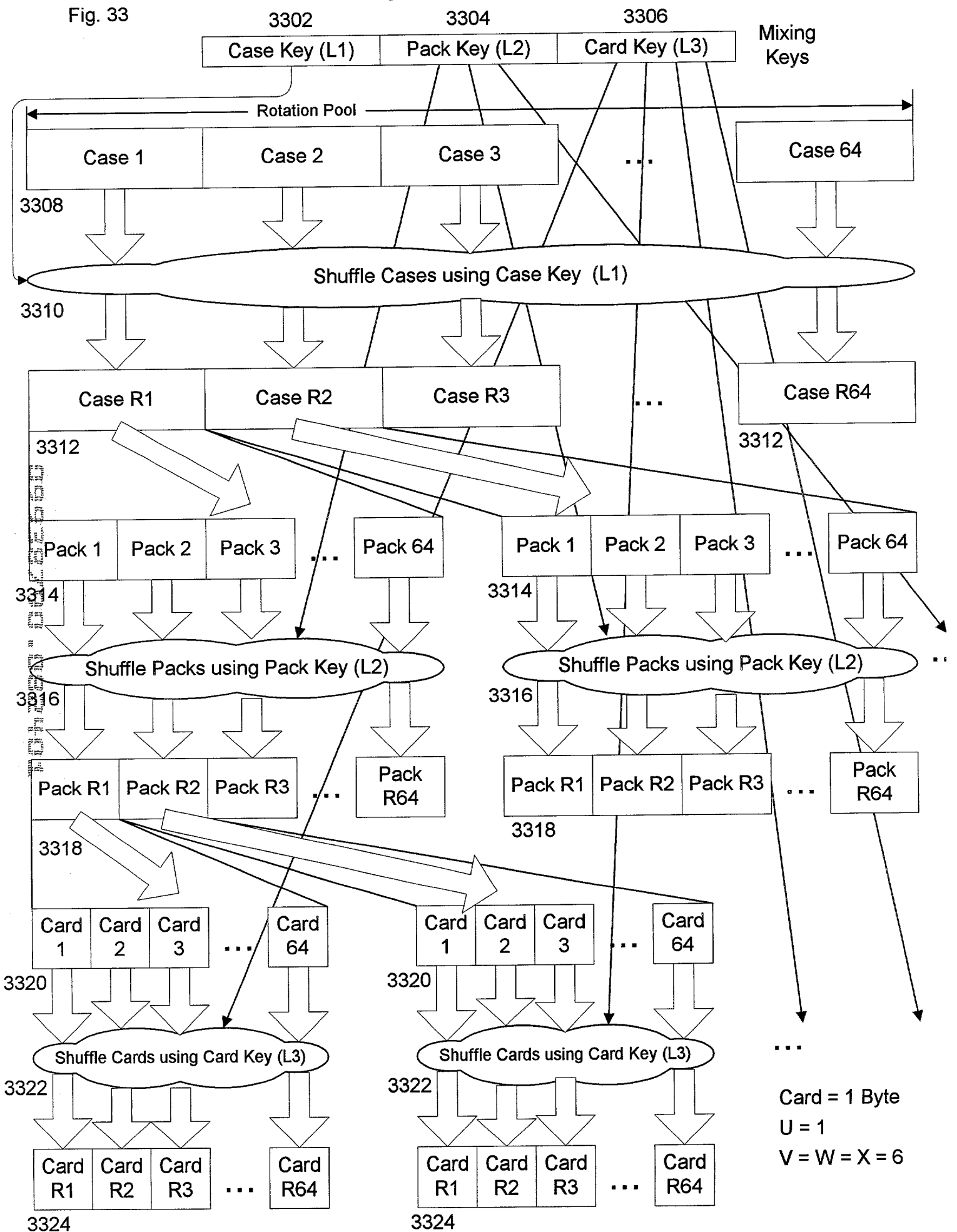


Fig. 34

